# Multi role IP Node
# KATABAMI Box

2020年10月（初版）
2020年10月（0.3版）
2020年10月（社外向け 0.3版）

株式会社SYNCHRO　中村 健

# KATABAMI とは？
## 特徴 と 対応方法

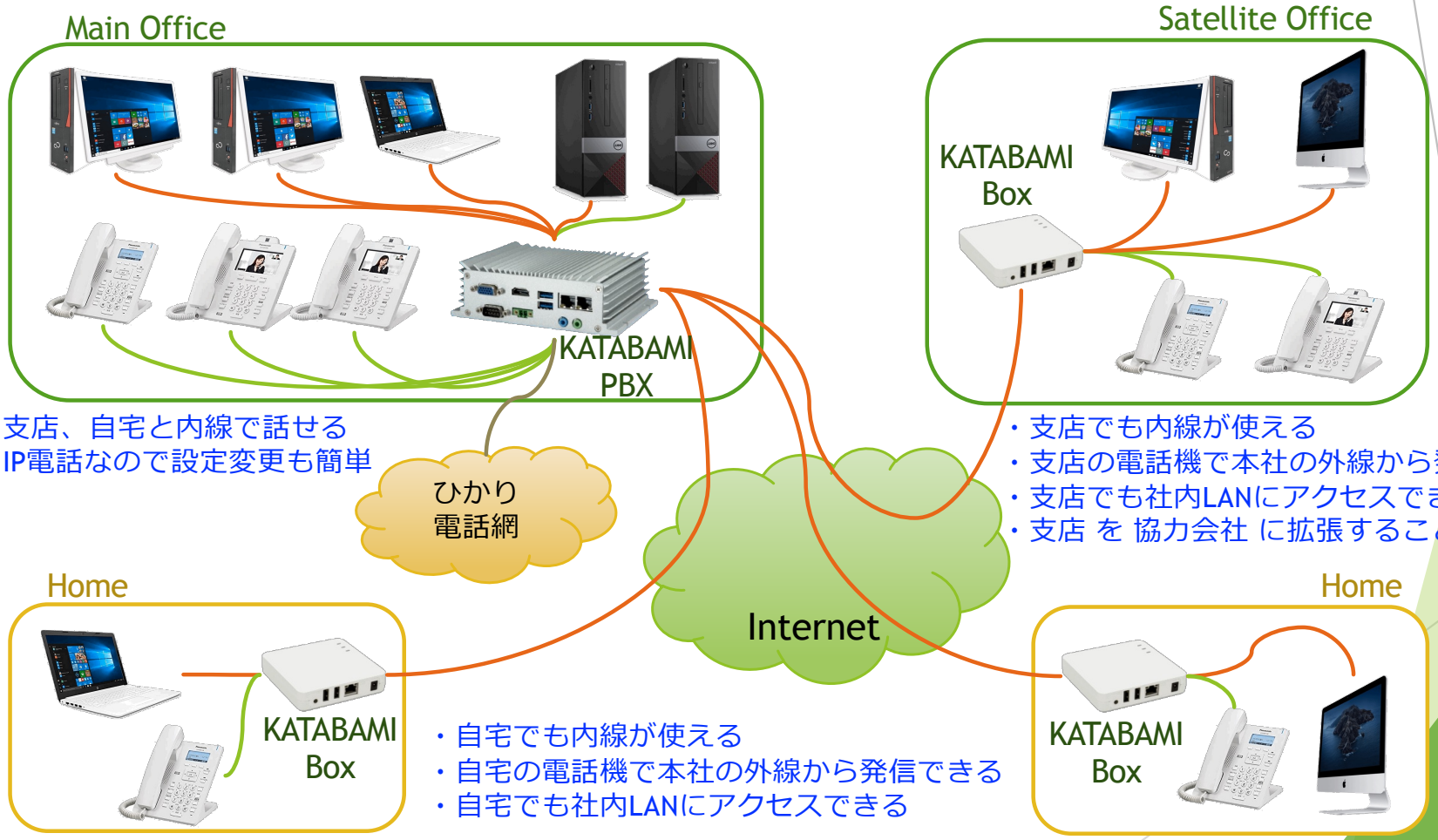
- KATABAMI の 特徴
  - 「なりすまし」を 絶対に 許さない
    - 通信する相手が、確かに 自分が接続を意図した End Point であることを保証
  - 通信データを 完全に 保護する
    - 自身と通信先の End Point 以外で 通信データを参照/操作できない ことを保証
    - ネットワークを保護する＝境界型 ではなく Zero Trust Security を実現
- KATABAMI 化
  - 真の Zero Trust Security を実現するには、KATABAMI の End Point への実装 が必要
  - KATABAMI を install
    - PC (Windows, MacOS）、サーバ (Linux, Windows Server)、スマホ (Android)
    - IPv6 で 通信可能な アプリケーションは、無改造で KATABAMI化
      - Webブラウザ、リモートデスクトップ 等々
      - Web会議サーバ、ビジネスチャットサーバ、画像サーバ、ファイルサーバ 等々
  - KATABAMI を 組み込み
    - KATABAMI Camera Series、KATABAMI Access、KATABAMI PBX Series

# KATABAMI Box
## 適用場面

- なんでも KATABAMI
  - KATABAMI化できない 装置 や アプリケーション を KATABAMI化
  - KATABAMI化できないケース とは？
    - 既存の IPデバイス
      - 例えば、IP Camera、IP電話機、スマートスピーカ、スマートメータ 等々
    - IPv6 未対応のアプリケーション
      - 例えば、人事管理システム、会計システム 等々
- Internet経由でも KATABAMI
  - IPv4 を 使って KATABAMI の 通信をトンネリング
    - Internet区間は、汎用性の高い IPv4 で接続
  - グローバル IPアドレス の取得が面倒な場合は KATABAMI Bridge
    - KATABAMI Bridge は SYNCHRO が提供する接続サービス
    - 固定グローバルIP をお持ちのの場合は、それを利用することも可能

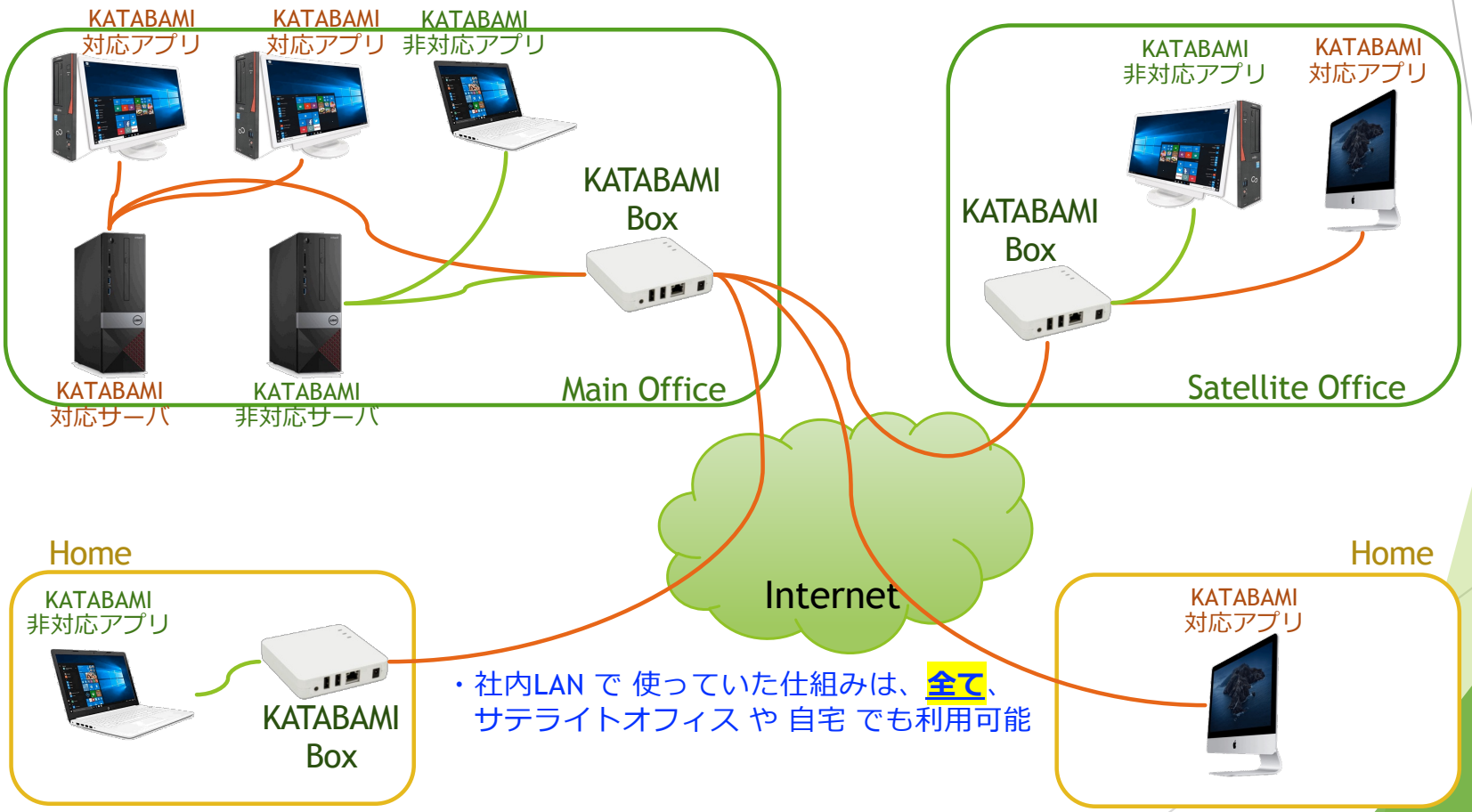
# KATABAMI Box 適用例

## KATABAMI で テレワーク環境構築



# KATABAMI Box 適用例

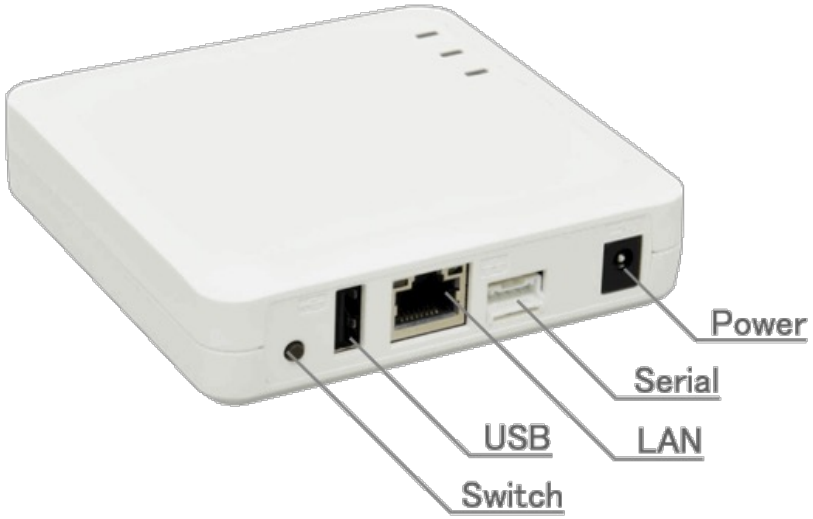
## KATABAMI 対応/非対応 の アプリケーション混在



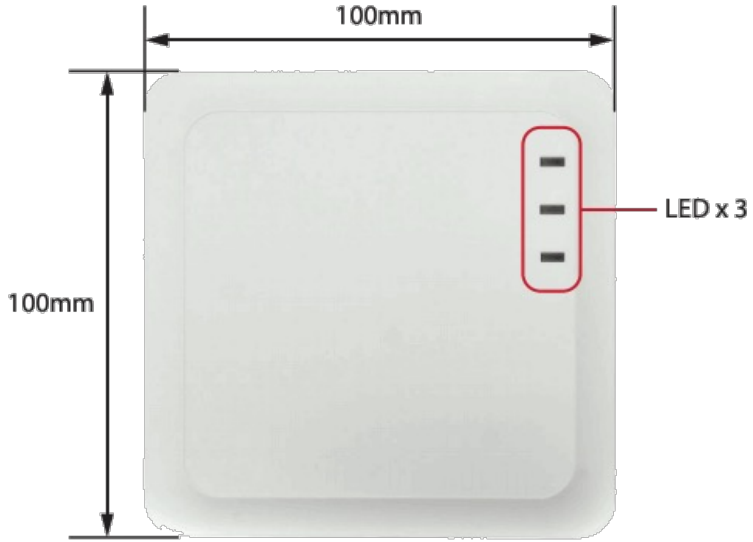

・社内LAN で 使っていた仕組みは、**全て**、
サテライトオフィス や 自宅 でも利用可能

# KATABAMI Box

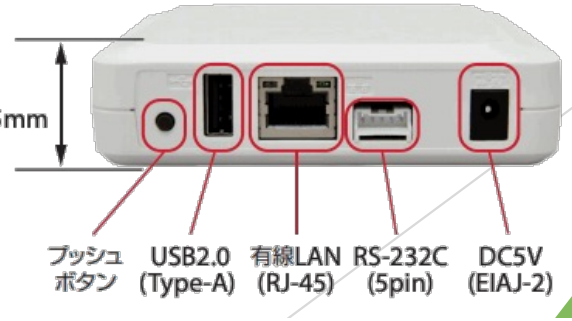
## 外観




● トップ面




● インタフェース面（側面）



# KATABAMI Box
## 仕様諸元

*基本仕様*

| | |
|---|---|
| 動作環境条件 | 温度条件:0~+40℃<br>湿度条件:20~80%RH(結露なきこと) |
| 保存環境条件 | 温度条件:-10~+50℃<br>湿度条件:20~90%RH(結露なきこと) |
| 電源 | AC100Vアダプタ |
| 外形寸法 | 100×100×25.5mm |
| 重量 | 118g(本体のみ) |
| 同梱物 | 本体、ACアダプタ |
| 各種取得規格 | VCCI Class-B、FCC Class B、ICES Class B<br>RoHS指令(EU)2015/863 |

*インターフェース仕様*

| | |
|---|---|
| 有線LANインタフェース | RJ-45:×1<br>10Base-T / 100Base-TX / 1000Base-T(自動認識) |
| 無線LANインタフェース | IEEE802.11a/b/g/n 2Tx2R<br>2.4GHz:Channel:1~13ch<br>5.xGHz:Channel:36~48・52~64・100~140ch |
| デバイスインタフェース | USB:×1(USB2.0 Hi-Speed Type-A)、シリアル:×1(5pin) |
| スイッチ | プッシュスイッチ:×1 |
| LED | 本体:×3 RJ-45:×2 |

# Appendix 1
## Zero Trust Security

- Zero Trust Security とは
  - 2019年辺りから 流行りだした。M社、C社 の propaganda が火付け役？
  - 2010年に Forrester Research社 が提唱した考え方
  - 決して信頼せず、常に確認する
    - 誰も & 何も、無条件には信用しない という考え方（少し切ない..？）
    - 全てのアクセス要求は、認証、承認、暗号化が行われてから許可される
  - どこでも 安心 しない（境界線の中を守るという発想は止める）
    - オープンな Internet 区間だけでなく、LAN 内でも警戒を怠らない
    - ファイアーウォールで守られていても、その内側に悪者がいるかも知れない
  - デメリットは 利便性の阻害 （そこで、KATABAMI の出番 というストーリ展開）
- Zero Trust Security ⇒ KATABAMI (“Zero Trust Security “ implies “KATABAMI”)
  - KATABAMI は ネットワーク層で Zero Trust Security の要件を充足
    - ペア鍵による認証（認証）
    - 接続相手の IPv6 address の正当性の確認（承認）
    - 楕円曲線暗号、ストリーム暗号の適用（暗号化）
  - さらに、アプリケーション層での認証や権限管理を行う

# Appendix 2
## トンネリング（tunneling）、IPv4 tunneling

- トンネリング とは
  - ある方式（プロトコル）での通信を、別の通信に載せて行うこと
  - 例えば..
    - 自転車で駅に行き、自転車を電車に載せて、下りた駅で自転車に乗る
    - この場合、自転車 を 電車 で トンネリング していることになる
- IPv4 tunneling とは
  - IPv4 を KATABAMI の通信で tunneling
    - Internet を経由する場合は、KATABAMI を IPv4 で tunneling
  - 利点 は 適用範囲の拡大 = 世の中の多くの機器やシステムは IPv4 で動いている
  - KATABAMI化できない モノを 無改修で KATABAMI化 する方法が KATABAMI の IPv4 tunneling